Overbroad Subpoena for Airbnb User Data Smacks of a General Warrant

by G.S. Hans [1]
November 6, 2013

For those who want to open their homes or spare rooms to guests, Airbnb has quickly become a popular option. Hosts advertise a room or their entire home on the site and guests can select available locations to stay for short periods of time. For guests, the options are often more affordable and flexible than a hotel – in some cases allowing for guests to cook or bring pets. I used Airbnb when my best friend and I went to Montreal a few months ago, and we had a fantastic experience.

Not everyone is taking so kindly to the service. Hotels and landlords have claimed that use of Airbnb can violate rental agreements and local hotel occupancy laws. These complaints are reminiscent of those that have frustrated services like Uber, the popular smartphone app that allows users to hail cars and pay using a linked credit card, which has angered taxi and limousine drivers. Like those services, Airbnb is a disruptive entrant into an established market full of entrenched actors.

However, Airbnb is now facing a challenge that raises serious issues of privacy and overreaching by government. Earlier this year, the New York Attorney General's office served a subpoena [2] requesting data on all Airbnb hosts who live in New York City in order to determine whether *any* hosts were violating a 2010 state law that prevents renters from subletting their units for under 30 days. While the New York state government has an obligation to enforce the laws on the books, the use of an overbroad subpoena to achieve that end is worrisome and a poor policy decision.

The NY Attorney General's subpoena demonstrates the danger of government agencies requesting data sets with an extremely broad interpretation of the relevance standard. Airbnb has approximately 225,000 users in New York. However, as reported in the *Daily News* [2], only about 15,000 of those are hosts – Airbnb users that offer places to stay – who could conceivably be violating the law. A subpoena that requests information about every *host* in order to find a few malfeasant actors is an invasive and unnecessary method of enforcing legal compliance.

What makes this particular incident especially problematic is the type of the data sought by the Attorney General. Airbnb user data contains names, addresses, email addresses, rates, and duration of specific stays. If Airbnb provided all this data pursuant to the subpoena, the government would amass a vast trove of sensitive data that would provide a high amount of information about the users' movements (most of which, presumably, involve stays outside New York). Across the entire Internet economy, consumers should be able to feel confident that the sensitive data they store with service providers is kept private and not released to the government in bulk. Should this type of broad subpoena become common practice, consumers and service providers may be reluctant to use or develop potentially useful services. Enforcement actions enabled by overbroad subpoenas will chill innovators from entering markets where incumbents have near-total control.

Indeed, it appears that the subpoena has already had chilling effects upon Airbnb's host user base [3], some of whom are struggling to make ends meet and many of whom enjoy the enriching social interactions that can occur between vacationers and hosts. Overbroad government access to data would imperil an even broader range of tangible and intangible benefits.

Airbnb has pledged to ensure that its hosts pay applicable taxes and has offered to work with regulatory authorities [4] to determine what laws apply and how to ensure that its users comply with those laws. A more targeted approach would be to craft a narrower subpoena that sought data only on hosts rather than all users and that further developed parameters intended to identify only hosts whose pattern of activity suggested a violation of the law.

In this age of "big data," we face a serious risk that government officials, from the National Security Agency to a state attorney general, will seek large data sets without even trying to narrow their

demands merely because the technology makes it so easy to compile and transfer data. Courts need to narrowly interpret the concept of relevance, and legislators need to impose limits on the powers they grant to ensure that data disclosure demands are narrowly targeted.

Source URL:
https://cdt.org/blogs/gs-hans/0611overbroad-subpoena-airbnb-user-data-smacks-general-warrant

Links:
[1] https://cdt.org/personnel/gs-hans
[2] http://www.nydailynews.com/news/national/state-airbnb-article-1.1477934#ixzz2h2So0ApS
[3] http://nymag.com/daily/intelligencer/2013/10/broke-creatives-now-afraid-to-host-on-airbnb.html
[4] http://publicpolicy.airbnb.com/fighting-for-you/